REMARKS

Applicants appreciate the thorough examination of the present application that is evidenced in the Official Action of July 12, 2005 (the "Official Action"). In response, Applicants have amended Independent Claims 1 and 33-35 and added new dependent claims 36-42. Applicants respectfully submit that the above-entitled application is now in condition for allowance for the reasons discussed below.

1. Status of the Claims

Claims 1-35 are pending in the present application. Claims 1-3 and 33-35 stand rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,175,917 to Arrow et al. ("Arrow"). Claim 4 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Arrow in view of U.S. Patent No. 5,931,928 to Brennan et al. ("Brennan"). Claims 5-6 and 11-29 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Arrow in view of U.S. Patent No. 6,094,485 to Weinstein et al. ("Weinstein"). Claims 7-8 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Arrow in view of Brennan and further in view of Weinstein. Claims 9-10 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Arrow in view of Brennan and further in view of Weinstein and U.S. Patent No. 5,764,738 to Gillon et al. ("Gillon"). Claims 30-32 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Arrow in view of Weinstein and further in view of Gillon.

2. The Independent Claims are Not Anticipated by Arrow

Claims 1 and 33-35 stand rejected under 35 U.S.C. § 102(e) as anticipated by Arrow. In response, Applicants have amended Independent Claims 1 and 33-35 as shown in the Listing of Claims. In particular, Independent Claim 1 has been amended as follows:

> 1. A method of performing security processing in a computing network comprising a local unit having an operating system kernel executing at least one application program, comprising:

receiving a first request at the operating system kernel from the application program to initiate a communication with a remote unit;

providing a second request from the operating system kernel to a security offload component which performs security handshake processing, the second request directing the security offload component to secure the communication with the remote unit; and

providing a control function in the operating system kernel for initiating operation of the security handshake processing by the security offload component. (emphasis added).

Similar amendments have been made to claims 33-35.

Arrow discloses a virtual private network (VPN) in which VPN units perform security management functions for VPN clients over a shared network. (See, e.g., Arrow, col. 5, l. 51 to col. 6, l. 23; and Arrow, col. 6, l. 62 to col. 7, l. 12.) It is instructive to note that in the system described by Arrow, the security processing is not controlled by the VPN client. Rather, the VPN units are controlled by a VPN management station 160 "through commands and configuration information transmitted to the respective VPN unit" through a public network. (Arrow, col. 6, ll. 31-34.) Thus, in the system of Arrow, VPN traffic is controlled according to instructions transmitted by a centralized VPN management station. While VPN systems may be useful for managing secure transactions among related clients over a public network, such systems may be distinguished from the present invention. For example, as stated in the present application:

> Another prior art offload technique involves a complete SSL security protocol offload from the system that is executing the server or client application. In this case, the offload device is inserted into the data path external to the endpoint communications system, and performs SSL security protocol processing on data in transit from or to the endpoint communications system. This technique uses less endpoint communications system resources than the other prior art technique, since all SSL security processing is offloaded, eliminating the two data bus crossings; however, there is no cooperation between the communications endpoint system and the offload device.

(App., p. 21, ll. 7-14.)

Amended Claim 1 recites, in part:

> receiving a first request at the operating system kernel from the application program to initiate a communication with a remote unit and providing a second request from the operating system kernel to a security offload component which performs security handshake processing, the second request directing the security offload component to secure the communication with the remote unit.

Similarly, Amended Claims 33-35 recite receiving a request at the operating system kernel from the application program to initiate a communication with a remote unit and directing the security offload component to secure the communication with the remote unit. In contrast, the security processing in the system of Arrow is transparent to the client (Arrow, col. 7, ll. 5-7). That is, in the system described by Arrow, security processing is performed based on source and destination addresses (Arrow, col. 6, ll. 62-67), rather than at the request of the client application. Thus, Arrow does not teach or suggest receiving a request at an operating system kernel from an application program to initiate a communication with a remote unit and directing a security offload component to secure the communication with the remote unit.

Furthermore, as the security processing functions of Arrow are performed entirely in the VPN unit under control of the VPN management station, Arrow fails to teach or suggest providing a control function in the operating system kernel for initiating operation of the security handshake processing by the security offload component as recited in Amended Claim 1. Accordingly, Applicants submit that Independent Claims 1 and 33-35 are patentable over Arrow for at least these reasons.

3. The Dependent Claims are Patentable Over the Cited Art

Dependent Claims 13, 15, 19 and 21 have been cancelled. New dependent claims 36-39 have been added. Applicants submit that dependent claims 2-12, 14, 16-18, 20, 22-32 and 36-39 are patentable at least as being dependent upon patentable base claims. Moreover, Applicants submit that many of the dependent claims are independently patentable. For example, with respect to claim 3, Applicants note that the "operating system kernel" recited in claim 3 refers to

an operating system kernel of a local unit which provides a request to a security offload component. In contrast, the "operating system 116" of Arrow refers to an operating system of the VPN. (See Arrow, Fig. 7 and col. 10, ll. 53-58.) Thus, Applicants submit that Arrow does not teach or suggest the limitations of dependent claim 3.

Further, Applicants submit that with respect to claims 4 and 7-10, the combination of Brennan with Arrow is improper. Brennan relates to data compression in a computer communication network (see, e.g., Brennan, Abstract). The Official Action alleges that the ordinary skilled person would have been motivated to apply the teaching of Brennan in the system of Arrow to let the offload security component take over the security handshake processing. (Official Action, pp. 4 and 7-10). Applicants respectfully submit, however, that neither Brennan nor Arrow includes any motivation or suggestion to combine their teachings as indicated in the Official Action.

As affirmed by the Court of Appeals for the Federal Circuit in In re Sang-su Lee, a factual question of motivation is material to patentability, and cannot be resolved on subjective belief and unknown authority. See In re Sang-su Lee, 277 F.3d 1338 (Fed. Cir. 2002). It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to "[use] that which the inventor taught against its teacher."

As noted above, Arrow is directed to a virtual private network in which security processing is performed by VPN units under control of a VPN management station. Brennan, on the other hand, discloses a system for negotiating data compression. The Office Action alleges that one skilled in the art would be motivated to combine Arrow and Brennan because such a combination would let the offload security component take over the security handshake processing. (Official Action, p. 4). Applicants respectfully submit that such reasoning with respect to whether a motivation exists to combine references is improper. As discussed above, the evidence of motivation to combine references must be clear and particular and must come from the prior art references, not from Applicants' disclosure. In the system of Arrow, security processing is performed by the VPN units in a manner that is transparent to the clients. Thus, in the system of Arrow, there is no handshake function to offload from the client. Offloading the security function from the VPN units would make the system of Arrow slower and more

complicated, since the VPN units of Arrow are already dedicated to performing security processing. Accordingly, there is no motivation to combine the teaching of Brennan with that of Arrow.

Applicants respectfully submit that the Official Action does not adequately address the issue of motivation to combine as discussed in In re Sang-su Lee. It appears that the Official Action finds a motivation to combine the cited references based on hindsight reasoning informed by Applicants' disclosure, which, as noted above, is an inappropriate basis for combining references. Accordingly, Applicants submit that claims 4 and 7-10 are patentable over Arrow in view of Brennan for at least these reasons.

Applicants further submit that new claims 36-39 are patentable over the art of record. For example, new claim 36 recites a method according to claim 1, further comprising preparing a data packet including data to be communicated to the remote unit; reserving space in the data packet for security protocol information; and passing the data packet including the reserved space to the security offload component. Applicants submit that, as the security processing functions of Arrow are performed transparently to the client, Arrow does not disclose or suggest the recitations of new claim 36, either alone or in combination with the other art of record.

Likewise, new claim 37 recites a method according to claim 36, further comprising passing control information from the operating system kernel to the security offload component, wherein the control information is passed to the security offload component in the space reserved in the data packet for security protocol information. New claim 38 recites a method according to claim 36, further comprising passing control information from the operating system kernel to the security offload component, wherein the control information is passed to the security offload component separately from the data packet. Applicants submit that the recitations of these claims are neither disclosed nor suggested by the art of record.

New claim 39 recites a method according to claim 36, further comprising receiving the data packet with the reserved space at the security offload component; encrypting the data in the data packet; inserting security protocol information in the reserved space; and transmitting the resulting data packet to the remote unit. Applicants submit that the recitations of new claim 39

are neither disclosed nor suggested by the art of record. Accordingly, Applicants respectfully submit that new claims 36-39 are patentable over the art of record.

CONCLUSION

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,

David C. Hall
Registration No. 38,904
Attorney for Applicants

Customer Number 46589
Myers Bigel Sibley & Sajovec, P.A.
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
919-854-1401 (Fax)